



CAPE

Réseaux Virtuels Sécurisés



Le problème

Depuis plus de 20 ans, la **sécurité réseau sur Internet évolue peu** et les attaques par déni de service et par usurpation d'identité continuent de croître. **L'absence d'identification et d'authentification des utilisateurs et de leurs machines** en est la cause principale. En effet, l'Internet est encore un espace largement ouvert et anonyme. Les services en ligne sensibles tels que les **banques**, les **services médicaux** et les **commerces** sont la cible privilégiée de cette faiblesse. Les **réseaux virtuels privés** permettent de sécuriser l'usage d'Internet mais ils ne sont actuellement **utilisables qu'au sein d'entités de taille restreinte** (e.g., une entreprise ou une institution). Il n'existe pas encore sur Internet de **réseaux virtuels publics** qui permettraient de **sécuriser les communications entre les entreprises et leurs clients, leurs fournisseurs ou leurs partenaires**.

Il y a un **besoin de zones sécurisées** (réseaux virtuels publics) dans lesquelles **l'identification et l'authentification des usagers et des services soit systématique et fiable** en se basant sur la cryptographie asymétrique. De telles zones permettraient de **réduire massivement l'envergure des cyber-attaques** sur les services situés à l'intérieur de celles-ci. En particulier, elles empêcheraient le hameçonnage puisque les attaquants ne pourraient plus créer de serveurs frauduleux au sein de ces zones.

Entre 2020 et 2021, les attaques cyber ont été **multipliées par quatre** selon un communiqué de la ministre des Armées du 4 mars 2021¹. Les entreprises et les institutions publiques doivent mobiliser des fonds importants en prévention et en réparation des attaques. Le marché de la cyber-sécurité a pesé \$150 milliards en 2019 et devrait dépasser \$300 milliards en 2027². La sécurité réseau coûte cher, soit directement (investissements en matériel, logiciel ou services) soit indirectement (coûts induits par des attaques, vol ou perte de données), et toute technologie permettant de réduire massivement les cyber-attaques est appelée à se développer dans le futur.

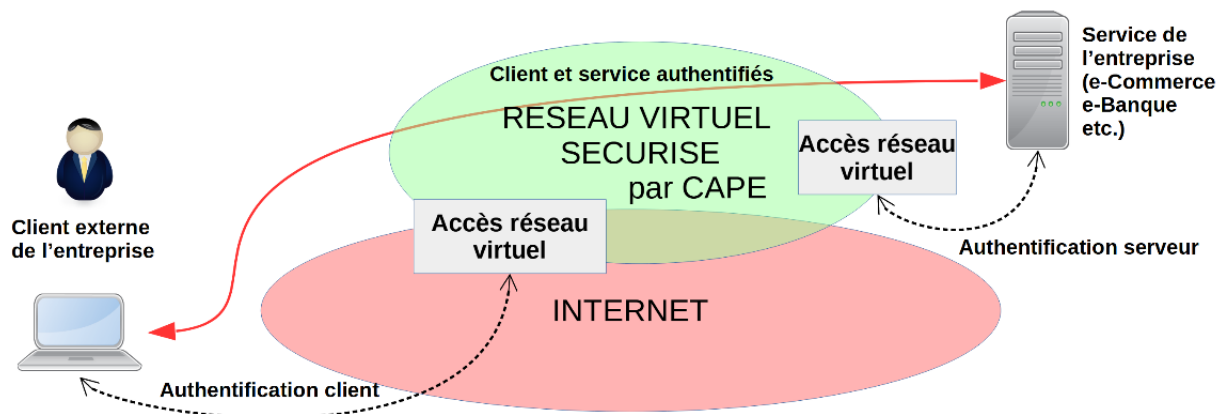
La solution CAPE

Nous souhaitons créer une entreprise fournissant un **service de création et de gestion de réseaux virtuels sécurisés entre les entreprises et leurs clients ou leurs partenaires**. Ce service s'appuiera sur un ensemble de technologies permettant la **création de réseaux isolés de l'Internet public** dans lesquels tous les participants (usagers et services) seront **identifiés et authentifiés** par l'usage de **cryptographie** à clé publique au niveau du réseau virtuel et au niveau des services.

Ainsi ces réseaux permettront de déployer des services en ligne commerciaux traitant des données sensibles, avec des **possibilités d'attaques bien plus faibles que dans l'Internet actuel**. Les entreprises et les institutions pourront utiliser notre service d'intermédiation afin de faire passer leurs clients et leurs partenaires par un réseau virtuel pour atteindre leurs services.

¹ https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/les-cyberattaques-ont-ete-multipliees-par-quatre-en-un-an-assure-la-ministre-florence-parly_4320225.html

² <https://www.alliedmarketresearch.com/cyber-security-market>



Dans ces réseaux virtuels, les flux de données sont définis par les **identifiants** des **usagers** et des **services** concernés ce qui permet, si besoin, de les **découpler** des appareils et des applications sur lesquels ils se trouvent afin de supporter la mobilité IP. De plus, l'authentification de ces entités (i.e., usagers et services) est effectuée par utilisation de **certificats** à clé publique. Ce modèle distribué, ne nécessite pas le stockage des informations d'identité en dehors des équipements appartenant à l'utilisateur.

Les facteurs différenciants

Concurrent	Réseau élastique	Authentification client par certificat	Gestion de la mobilité	Confiance (blockchain)
CAPE	✓	✓	✓	✓
Opérateurs VPN (Orange, ...)	✗	✗	✗	✗
Fournisseurs d'IDs (Otko, ...)	✗	✓	✗	✗
Hébergeurs SASE (Zscaler, ...)	✓	✓	✗	✗

Intérêt de la solution CAPE pour votre entreprise

Nous recherchons des entreprises ayant des services en ligne sensibles (e.g., transactions financières, données confidentielles) et qui souhaiteraient augmenter leur niveau de protection face aux cyber-attaques. Si vous êtes une telle entreprise et que vous possédez de nombreux clients ou partenaires externes, seriez-vous intéressé par notre proposition de valeur ou par certains aspects de celle-ci ? Si oui, nous serions ravis de pouvoir **échanger** avec vous afin que vous puissiez exprimer vos **attentes** par rapport à la solution CAPE.

Contact Damien Magoni – damien@cape-cybersecurity.fr

Soutiens

